0500

P/2635-43

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Jun Kametani
Serial No:09/532,585
Filed:March 22, 2000
For: PACKET SWITCHING APPARATUS WITH HIGH SPEED ROUTING FUNCTION

Date: April 7, 2000
Group Art Unit:

Assistant Commissioner for Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

In accordance with 35 U.S.C. §119, Applicant confirms the request for priority under the International Convention and submits herewith the following document in support of the claim:

Certified Japanese Registration No.
11-098140 Filed April 5, 1999

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on April 7, 2000:

Steven I. Weisburd
Name of applicant, assignee or Registered Representative

Signature
April 7, 2000
Date of Signature

Respectfully submitted,

Steven I. Weisburd
Registration No.: 27,409
OSTROLENK, FABER, GERB & SOFFEN, LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700

SIW:dr1

US

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ４月 ５日

出 願 番 号
Application Number: 平成１１年特許願第０９８１４０号

出 願 人
Applicant (s): 日本電気株式会社

２０００年 ３月１０日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆

出証番号 出証特２０００－３０１４２８４

【書類名】　特許願

【整理番号】　47201392

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/00

H04L 12/00

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　亀谷　潤

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100093595

【弁理士】

【氏名又は名称】　松本　正夫

【手数料の表示】

【予納台帳番号】　057794

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　パケット交換装置

【特許請求の範囲】

【請求項１】　パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、

ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、

前記マイクロプロセッサによりルーティング処理がなされたパケットに関して、ＩＰ発信元アドレスとＩＰ宛先アドレスとをサーチキーとして、ルーティング処理の結果を登録し、保持するＩＰフローテーブルと、

パケットを受信した場合に、該受信パケットのＩＰ発信元アドレス及びＩＰ宛先アドレスをサーチキーとして前記ＩＰフローテーブルを検索し、検索の結果、該当するＩＰフローが登録されていた場合、前記マイクロプロセッサによるルーティング処理へ移行することなく、該ＩＰフローに示されるルーティング処理結果に基づいて、該パケットを適切な出力ポートへ転送するパケット処理実行手段と、

ネットワークインタフェースと接続され、受信したパケットに対して下位レイヤの処理を実行して前記パケット手段に転送し、前記パケット手段から受け取ったパケットに対して下位レイヤの処理を実行してネットワークへ送出する下位レイヤ処理手段と

を備えることを特徴とするパケット交換装置。

【請求項２】　パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段をさらに備え、

前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、

前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行すること

を特徴とする請求項１に記載のパケット交換装置。

【請求項３】　前記ＩＰフローテーブルが、前記ルーティング処理の結果に加えて、前記マイクロプロセッサによって決定された前記セキュリティ情報を登録し、

前記パケット処理実行手段が、前記受信パケットのＩＰ発信元アドレス及びＩＰ宛先アドレスをサーチキーとして前記ＩＰフローテーブルを検索した結果、該当するＩＰフローが登録されておりかつ該ＩＰフローエントリに前記セキュリティ情報が登録されていた場合に、前記マイクロプロセッサによる前記セキュリティ情報の取得処理へ移行することなく、該ＩＰフローに示される前記セキュリティ情報と共に前記受信パケットを前記セキュリティ処理手段に送り、

前記セキュリティ処理手段が、前記パケット処理実行手段から受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする請求項２に記載のパケット交換装置。

【請求項４】　前記マイクロプロセッサと前記パケット処理実行手段とがプロセッサバスを介して接続されており、前記パケット処理実行手段と前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする請求項２または請求項３に記載のパケット交換装置。

【請求項５】　前記パケット処理実行手段が、前記セキュリティ処理手段により暗号化処理を施されるパケットを、該パケットを転送先のパケット装置との間で用いられる通信パケットでカプセル化することを特徴とする請求項２または請求項３に記載のパケット交換装置。

【請求項６】　パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、

ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、

パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段と、

ネットワークインタフェースと接続され、パケットの送受信を行うと共に、受信したパケット及び送信するパケットに対して下位レイヤの処理を実行する下位レイヤ処理手段とを備え、

前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、

前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行すること

を特徴とするパケット交換装置。

【請求項７】　前記マイクロプロセッサと前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする請求項６に記載のパケット交換装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、パケット通信ネットワークにおいて用いられるパケット交換装置に関し、特にマイクロプロセッサの負担を軽減してルーティング処理の高速化を図ったパケット交換装置に関する。

【０００２】

【従来の技術】

インターネットに代表されるパケット通信ネットワークでは、パケット単位でデータの伝送が行われる。パケットにはデータの発信元や宛先のアドレス等に関する情報を含むヘッダが付されており、ルータ等のパケット交換装置が、当該ヘッダ部分のアドレス情報に基づき、パケット単位で適切なネットワークへと転送する。

【０００３】

従来、パケットのルーティング処理は、パケット単位でのルーティング処理と

いう仕組みのため、ソフトウェアで実装されることが多かった。パケットのルーティング処理を実行する従来のパケット交換装置の構成を図９に示す。図９に示すパケット交換装置は、データリンク層以下の処理をハードウェアで実行する下位レイヤ処理部１１０と、マイクロプロセッサ１０１、マイクロプロセッサ１０１上のソフトウェアやルーティング情報を格納するためのメインメモリ１０２、受信したパケットを格納しておくパケットメモリ１０５、および下位レイヤ処理部１１０とパケットメモリ１０５の間でパケットデータを転送するためのＤＭＡコントローラ１１２を備える。

【０００４】

図９に示すように構成された従来のルータにおいてパケットを受信すると、ＤＭＡコントローラ１１２が、一旦、受信した当該パケットを下位レイヤ処理部１１０からパケットメモリ１０５に転送しておく。この後、マイクロプロセッサ１０１が、プロセッサバス１０３を経由してパケットメモリ１０５上のパケットをメインメモリ１０２にコピーする。そして、ソフトウェア制御によりルーティング処理を行い、当該処理によってＭＡＣヘッダを付替えたパケットを、再びパケットメモリ１０５にコピーする。次に、ＤＭＡコントローラ１１２が、当該処理済パケットを出力物理ポートに接続する下位レイヤ処理部１１０へと転送し、下位レイヤ処理部１１０による処理の後にネットワークへと送信される。

【０００５】

以上のように、従来のパケット交換装置は、全ての受信パケットに対するルーティング処理を、ソフトウェア制御によりマイクロプロセッサ１０１が行うため、ネットワーク速度はマイクロプロセッサ１０１自身の性能に依存していた。

【０００６】

ところで、パケット通信方式は、回線交換方式に比べデータのセキュリティが弱いことが従来から指摘されている。また、近年のインターネットの急激な普及により、パケット通信におけるセキュリティ対策が急務となった。そこで、ネットワークレイヤでのセキュリティ対策として、ＩＰパケットデータを暗号化する方式（ＩＰｓｅｃ）が標準化された。従来のパケット交換装置においては、当該ＩＰｓｅｃによるパケットデータの暗号化／復号化処理もマイクロプロセッサ１

０１が全て行っていた。

〔０００７〕

〔発明が解決しようとする課題〕

上述したように、従来のパケット交換装置は、全ての受信パケットに対するルーティング処理を、ソフトウェア制御によりマイクロプロセッサが行っていたため、ネットワーク速度はマイクロプロセッサ自身の性能に依存していた。したがって、通信トラヒックの増加やネットワーク速度の高速化の要請に対して、マイクロプロセッサの性能による限界があるという欠点があった。

〔０００８〕

図９に示したパケット交換装置において、パケットメモリ１０５とメインメモリ１０２とを同一のメモリ素子にて構成することにより、メモリ間のデータ転送に要する時間を短縮することが可能である。しかし、依然としてパケット毎の処理は全てマイクロプロセッサの負荷となるため、処理の高速化に対してマイクロプロセッサの性能による限界があるという欠点は解決されない。

〔０００９〕

また、パケット通信におけるセキュリティを向上させるため、従来のパケット交換装置に、上述したＩＰｓｅｃによるパケットデータの暗号化／復号化処理を実装する場合、当該処理を実行するためにマイクロプロセッサの能力を割かれるため、パケット交換装置における全体的な処理性能が低下し、処理の高速化に対する限界をさらに引き下げるという欠点があった。

〔００１０〕

具体的には、上記従来のパケット交換装置に、ＩＰｓｅｃ処理を新たに追加した場合、パケットのデータスループットが約１０分の１にまで低下する場合があった。

〔００１１〕

本発明は、上記従来の欠点を解決し、ルーティング処理及びセキュリティ処理におけるマイクロプロセッサの負担を軽減することにより、パケット交換処理の高速化を実現するパケット交換装置を提供することにある。

〔００１２〕

【課題を解決するための手段】

上記の目的を達成する本発明は、パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、前記マイクロプロセッサによりルーティング処理がなされたパケットに関して、ＩＰ発信元アドレスとＩＰ宛先アドレスとをサーチキーとして、ルーティング処理の結果を登録し、保持するＩＰフローテーブルと、パケットを受信した場合に、該受信パケットのＩＰ発信元アドレス及びＩＰ宛先アドレスをサーチキーとして前記ＩＰフローテーブルを検索し、検索の結果、該当するＩＰフローが登録されていた場合、前記マイクロプロセッサによるルーティング処理へ移行することなく、該ＩＰフローに示されるルーティング処理結果に基づいて、該パケットを適切な出力ポートへ転送するパケット処理実行手段と、ネットワークインタフェースと接続され、受信したパケットに対して下位レイヤの処理を実行して前記パケット手段に転送し、前記パケット手段から受け取ったパケットに対して下位レイヤの処理を実行してネットワークへ送出する下位レイヤ処理手段とを備えることを特徴とする。

【００１３】

請求項２に記載の本発明のパケット交換装置は、パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段をさらに備え、前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする。

【００１４】

請求項３に記載の本発明のパケット交換装置は、前記ＩＰフローテーブルが、前記ルーティング処理の結果に加えて、前記マイクロプロセッサによって決定された前記セキュリティ情報を登録し、前記パケット処理実行手段が、前記受信パ

ケットのＩＰ発信元アドレス及びＩＰ宛先アドレスをサーチキーとして前記ＩＰフローテーブルを検索した結果、該当するＩＰフローが登録されておりかつ該ＩＰフローエントリに前記セキュリティ情報が登録されていた場合に、前記マイクロプロセッサによる前記セキュリティ情報の取得処理へ移行することなく、該ＩＰフローに示される前記セキュリティ情報と共に前記受信パケットを前記セキュリティ処理手段に送り、前記セキュリティ処理手段が、前記パケット処理実行手段から受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする。

〔００１５〕

請求項４に記載の本発明のパケット交換装置は、前記マイクロプロセッサと前記パケット処理実行手段とがプロセッサバスを介して接続されており、前記パケット処理実行手段と前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする。

〔００１６〕

請求項５に記載の本発明のパケット交換装置は、前記パケット処理実行手段が、前記セキュリティ処理手段により暗号化処理を施されるパケットを、該パケットを転送先のパケット装置との間で用いられる通信パケットでカプセル化することを特徴とする。

〔００１７〕

請求項６に記載の本発明のパケット交換装置は、パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、パケットの暗号化処理及び復号化処理を専用のハードウェアによって行うセキュリティ処理手段と、ネットワークインタフェースと接続され、パケットの送受信を行うと共に、受信したパケット及び送信するパケットに対して下位レイヤの処理を実行する下位レイヤ処理手段とを備え、前記マイクロプロセッサが、所定の規則に基づいてパケットを暗号化または復号化すべきと判断した場合に、セキュリティ情報として暗号化または復号化の処理方式

及び該処理に要する暗号鍵を決定して、前記セキュリティ処理手段に通知し、前記セキュリティ処理手段が、前記マイクロプロセッサから受け取ったセキュリティ情報に基づいてパケットの暗号化処理または復号化処理を実行することを特徴とする。

〔００１８〕

請求項７に記載の本発明のパケット交換装置は、前記マイクロプロセッサと前記下位レイヤ処理手段とが所定のスイッチファブリックを介して接続されており、かつ前記セキュリティ処理手段が前記下位レイヤ処理手段と同一のスイッチファブリックに接続されていることを特徴とする。

〔００１９〕

〔発明の実施の形態〕

以下、本発明の実施の形態について図面を参照して詳細に説明する。

〔００２０〕

図１は、本発明の一実施形態によるパケット交換装置の構成を示すブロック図である。図１を参照すると、本実施形態のパケット交換装置は、マイクロプロセッサ１１と、メインメモリ１２と、マイクロプロセッサ１１とメインメモリ１２やその他の周辺処理部とを接続するためのプロセッサバス１３と、マイクロプロセッサ１１に代わってパケット処理を実行するためのパケット処理部１４、パケットメモリ１５、サーチ処理部１６及びＩＰフローテーブル１７と、パケットの暗号化／符号化処理を行うセキュリティ処理部１９と、下位レイヤ処理部２０と、パケット処理部１４とセキュリティ処理部１９と下位レイヤ処理部２０とを相互に接続するためのスイッチファブリック１８とを備える。なお、図１には、本発明における特徴的な構成のみを記載し、他の一般的な構成については記載を省略してある。

〔００２１〕

上記構成において、マイクロプロセッサ１１は、ソフトウェア制御によりパケット交換装置全体の制御を行うと共に、受信パケットの転送先を決めるルーティング処理や、必要に応じてパケットデータに対する暗号化または復号化の必要性を判断する処理を行う。

〔００２２〕

メインメモリ１２は、マイクロプロセッサ１１を制御するソフトウェアや、所定の処理を行う際に当該処理に関わる各種データを格納する。

〔００２３〕

パケット処理部１４は、ネットワークインタフェースから受信したパケットに対して、ＩＰヘッダ処理や出力先ネットワークインタフェースへの転送処理を行う。ここで、ＩＰヘッダ処理とは、パケットに付加されているヘッダからＩＰ宛先アドレスやＩＰ発信元アドレスを抽出する処理、マイクロプロセッサ１１によるルーティング処理によって決定されたＭＡＣアドレスに応じて新しいＭＡＣヘッダを生成する処理等を含む。

〔００２４〕

また、パケット処理部１４は、パケットヘッダから抽出したサーチキーによりサーチ処理部１６を制御してＩＰフローテーブル１７を検索させたり、ＩＰフローテーブル１７に新しいＩＰフローを仮登録させたりする。また、サーチ処理部１６によるＩＰフローテーブル１７の検索結果に応じて、取得した出力物理ポートやＭＡＣアドレスに基づき、該当パケットのＩＰヘッダ処理を行う。

〔００２５〕

パケットメモリ１５は、マイクロプロセッサ１１やパケット処理部１４による処理のために受信パケットを一時的に格納する。また、マイクロプロセッサ１１がルーティング処理を行う際に処理結果を待つパケットを登録するプロセッサ処理結果待ちキューを有する。

〔００２６〕

サーチ処理部１６は、パケット処理部１４からの指示にしたがって、ＩＰフローテーブル１７を検索し、登録されている該当パケットに関するルーティング処理の結果をパケット処理部１４に返す。また、パケット処理部１４からの指示に対応するＩＰフローエントリが存在しない場合、当該指示に基づいてＩＰフローの仮登録を行う。さらに、マイクロプロセッサ１１によるルーティング処理の結果を受け取って、仮登録のＩＰフローエントリに格納し、当該ＩＰフローを正式登録する。

〔００２７〕

ＩＰフローテーブル１７は、ＩＰ発信元アドレスとＩＰ宛先アドレスとをサーチキーとして、マイクロプロセッサ１１によるルーティング処理の結果であるＩＰフローを格納したテーブルである。図２にＩＰフローテーブル１７の例を示す。図２を参照すると、ＩＰフローテーブル１７には、ＩＰフローエントリごとに、サーチキーであるＩＰ発信元アドレス及びＩＰ宛先アドレスと、ルーティング処理の結果であるＭＡＣ発信元アドレス、ＭＡＣ宛先アドレス及び出力物理ポートのポート番号とが登録されている。また、必要に応じて、後述するセキュリティ情報が格納されている。

〔００２８〕

スイッチファブリック１８は、複数のネットワークインタフェースと個別に接続された複数の下位レイヤ処理部２０と、パケット処理部１４と、セキュリティ処理部１９とを相互に接続する。スイッチファブリック１８としては、接続された各ユニット間のデータ転送時の調停機能やアドレッシング機能を持っていれば何でも良く、単純なＴｒｉ－ｓｔａｔｅバス、リングバス、クロスバススイッチなど実現手段は問わない。また、スイッチファブリック１８の構成をトークンリングバス構成としても良い。

〔００２９〕

セキュリティ処理部１９は、マイクロプロセッサ１１によるソフトウェア処理に基づき、必要に応じて、パケット毎に暗号化／復号化処理を実行する。

〔００３０〕

下位レイヤ処理部２０は、物理的なネットワークインタフェースと接続され、データリンク層（ＯＳＩ７レイヤモデルの第２層）以下の処理を実行し、スイッチファブリック１８を介してパケット処理部１４との間でパケットの送受信を行う。

〔００３１〕

以上、本実施形態の構成を説明したが、実際には、本実施形態のパケット交換装置は上記各構成要素の機能を実現する各種の回路にて構成され、例えば、上記各構成要素を内包する半導体集積回路にて構成しても良い。

〔００３２〕

次に、図３乃至図７のフローチャートを参照して本実施形態の動作について説明する。図３は、本実施形態によるパケット処理の主要な流れを示すフローチャートである。図４は、マイクロプロセッサ１１によるルーティング処理の流れを示すフローチャートである。図５乃至図７は、セキュリティ処理を伴う場合の本実施形態によるパケット処理の流れを示すフローチャートである。

〔００３３〕

本実施形態のパケット交換装置は、インターネットに代表されるパケット通信のネットワークレイヤの処理を行う装置であるため、ネットワークインタフェースより受信したパケットのヘッダを解析し、その宛先アドレス（ＩＰ宛先アドレス）に基づくルーティング処理を行い、その結果にしたがって出力先のネットワークインタフェースへパケットを転送する動作が基本となる。加えて、本実施形態では、受信パケットのルーティング処理の際にＩＰ宛先アドレスとＩＰ発信元アドレスに基づき、必要に応じて、パケット単位にデータの暗号化／復号化等のセキュリティ処理を併せて実行する。したがって、以下の動作の説明では、先に通常のセキュリティ処理を実施しない場合の動作について説明し、次にセキュリティ処理を実行する場合の動作を説明する。

〔００３４〕

図３を参照すると、まず、パケット交換装置の外部のネットワークと接続された下位レイヤ処理部２０に外部装置からパケットが到着すると（ステップ３０１）、当該下位レイヤ処理部２０は、レイヤ２以下のパケット処理、すなわちデータの同期確立、下位レイヤヘッダ（ＭＡＣヘッダ等）の検証、ＣＲＣの検算等を実行する（ステップ３０２）。そして、下位レイヤの処理を終えたパケットを、スイッチファブリック１８を経由してパケット処理部１４へと転送する。

〔００３５〕

パケット処理部１４は、転送された受信パケットを受け取ると、まず当該パケットをパケットメモリ１５に格納する。そして、当該パケットのパケットヘッダからＩＰ宛先アドレスやＩＰ発信元アドレス等を抽出し、これらからＩＰフローテーブル１７を検索するためのサーチキーを作成する（ステップ３０３）。次に

、パケット処理部１４は、作成したサーチキーをサーチ処理部１６へ送り、ＩＰフローテーブル１７の検索を指示する。

〔００３６〕

サーチ処理部１６は、パケット処理部１４から受け取ったサーチキーを用いてＩＰフローテーブル１７の検索を行い、その結果をパケット処理部１４に通知する（ステップ３０４）。サーチ処理部１６による検索の結果、ＩＰフローテーブル１７に受信したパケットに相当するＩＰフローが登録されている場合、すなわち、マイクロプロセッサ１１により当該ＩＰフローに対応するパケットに対するルーティング処理が既に行われていた場合は、パケット処理部１４は、サーチ処理部１６から検索結果（図２に示すＩＰフローテーブル１７ではＭＡＣ発信元アドレス、ＭＡＣ宛先アドレス及び出力物理ポートのポート番号）を受け取り、当該情報に基づいて当該パケットのヘッダ処理を行う（ステップ３０５、３０６）。そして、当該情報が示す出力物理ポートに接続された下位レイヤ処理部２０へ当該パケットを転送する（ステップ３０７）。以上の動作により、当該パケットに関しては、ソフトウェア制御によるマイクロプロセッサ１１のルーティング処理を行うことなく、パケット処理部１４が自律的にパケットの転送を実行することができる。

〔００３７〕

下位レイヤ処理部２０は、スイッチファブリック１８を介してパケット処理部１４からパケットを受け取り、下位レイヤ固有の処理、すなわちパケット全体のＣＲＣ演算、及び当該演算結果をパケットに付加する処理を行って（ステップ３０８）、自身が接続されているネットワークインタフェースへ当該パケットを送出する（ステップ３０９）。

〔００３８〕

これに対し、サーチ処理部１６による検索の結果、ＩＰフローテーブル１７に受信したパケットに相当するＩＰフローが登録されていない場合、パケット処理部１４は、サーチ処理部１６に指示してＩＰ宛先アドレス及びＩＰ発信元アドレスをサーチキーとする新しいＩＰフローの仮登録を実行させる（ステップ３０５、３１０）。これは、図２のＩＰフローテーブルにおいて、サーチキーの項だけ

が存在するエントリに相当する。次に、パケット処理部１４は、マイクロプロセッサ１１に対して割り込みを掛けて、マイクロプロセッサ１１によるルーティング処理へ当該パケットを引き渡す（ステップ３１１）。そして、当該パケットをパケットメモリ１５のプロセッサ処理結果待ちのキューに登録した後、パケット処理部１４は、次のパケットの処理へと移行する（ステップ３１２）。

〔００３９〕

この後、パケット処理部１４は、新たに受信したパケット処理の合間に、パケットメモリ１５のプロセッサ処理結果待ちキューのパケットを調べ、キューの先頭に置かれたパケットのサーチキーを作成し、サーチ処理部１６を制御してＩＰフローテーブル１７の検索を実行する（ステップ３１３）。後述するように、当該パケットに対するマイクロプロセッサ１１によるルーティング処理が完了したならば、該当するＩＰフローエントリは正式登録されており、検索結果としてＭＡＣ発信元アドレス、ＭＡＣ宛先アドレス及び出力物理ポートのポート番号が得られる（ステップ３１４）。そして、パケット処理部１４は、得られたＭＡＣアドレス及び出力物理ポートのポート番号に基づいて当該パケットのヘッダ処理を行う（ステップ３１５）。以下、パケットを下位レイヤ処理部２０へ転送し、下位レイヤ固有の処理の後、ネットワークインタフェースへ送出する（ステップ３０７、３０８、３０９）。

〔００４０〕

この後、同一のＩＰ発信元アドレス及びＩＰ宛先アドレスを有するパケットを受信した場合は、対応するＩＰフローがＩＰフローテーブル１７に登録されているため、ステップ３０５、３０６及び３０７の処理により、当該パケットに関して、ソフトウェア制御によるマイクロプロセッサ１１のルーティング処理を行うことなく、パケット処理部１４が自律的にパケットの転送を実行できることとなる。

〔００４１〕

次に、ステップ３１１により、マイクロプロセッサ１１によるルーティング処理へ当該パケットが引き渡された場合のマイクロプロセッサ１１の動作を説明する。図４を参照すると、マイクロプロセッサ１１は、パケット処理部１４からの

割り込みに応じてルーティング処理を開始し、まず、プロセッサバス１３及びパケット処理部１４を介してパケットメモリ１５にアクセスする（ステップ４０１）。そして、パケットメモリ１５のプロセッサ結果処理待ちキューから、登録されているパケットのヘッダ部分のみを、メインメモリ１２へコピーする（ステップ４０２）。

〔００４２〕

次に、マイクロプロセッサ１１は、コピーされたパケットヘッダ部のＩＰ宛先アドレスをキーとして、メインメモリ１２に予め格納されているＩＰルーティングテーブル及びＡＲＰキャッシュテーブルの検索を実行する（ステップ４０３）。そして、パケットの転送先となる出力物理ポート及びネクストホップのＭＡＣアドレスを決定する（ステップ４０４）。そして、これら一連のルーティング処理結果を、プロセッサバス１３及びサーチ処理部１６を介してＩＰフローテーブル１７に送り、仮登録済みのＩＰフローエントリの正式登録を行う（ステップ４０５）。この動作は、図２に示すＩＰフローテーブル１７の該当エントリに、ルーティング結果が追記されたことに相当する。

〔００４３〕

次に、パケット単位のセキュリティ処理を伴う場合の本実施形態の動作について説明する。セキュリティ処理として、ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）で定められたＩＰｓｅｃに対する処理を行う場合を例として説明する。

〔００４４〕

ＩＰｓｅｃをルータ等のパケット交換装置に実装する場合、パケットを転送したい相手先ホストが所属するネットワークに存在するパケット交換装置との間で、パケットの暗号化方式や暗号鍵の情報を予め共有し、そのパケットを当該パケット交換装置間どうしの通信パケットでカプセル化する方法（トンネルモード）を使用する。パケットの暗号化方式と暗号鍵の共有は通信するホスト間で一意であり、したがってパケット交換装置は、ＩＰ宛先アドレスとＩＰ発信元アドレスから、当該パケットに適用すべき暗号化方式と暗号鍵を決定できる。これらの共有情報は当該パケット交換装置どうしの間で事前に、または必要に応じて確立す

る必要がある。本実施形態では、共有情報の確立に付随する処理は全て、ソフトウェア制御によりマイクロプロセッサ１１が処理する。ＩＰｓｅｃトンネルモードによって処理されたＩＰパケットの構成を図８に示す。

〔００４５〕

本動作例において、パケット交換装置にパケットが到着してからＩＰフローがＩＰフローテーブル１７に仮登録され、マイクロプロセッサ１１によるルーティング処理へパケットが引き渡されるまでの処理は、図３に示した通常の動作と同様である（ステップ３０１～３０５、３１０、３１１参照）。

〔００４６〕

図５を参照すると、マイクロプロセッサ１１は、パケット処理部１４からの割り込みに応じてルーティング処理を開始し、まず、プロセッサバス１３及びパケット処理部１４を介してパケットメモリ１５にアクセスする（ステップ５０１）。そして、パケットメモリ１５のプロセッサ結果処理待ちキューから、登録されているパケットのヘッダ部分のみを、メインメモリ１２へコピーする（ステップ５０２）。

〔００４７〕

次に、マイクロプロセッサ１１は、コピーされたパケットヘッダ部のＩＰ宛先アドレスを識別する（ステップ５０３）。当該パケットが図８に示したようなＩＰｓｅｃヘッダを持つパケットであり、かつ当該ＩＰアドレスが自装置（パケット交換装置）のＩＰアドレスであるならば、ＩＰｓｅｃの復号化対象パケットとして認識する（ステップ５０４）。また、ＩＰアドレスが自装置のＩＰアドレスでないならば、ＩＰｓｅｃの暗号化対象パケットとして認識する（ステップ５０５）。

〔００４８〕

まず、図６を参照して、ＩＰｓｅｃ暗号化対象パケットに対する処理について説明する。この場合、マイクロプロセッサ１１は、パケットヘッダ部のＩＰ宛先アドレスをキーとして、メインメモリ１２に予め格納されているセキュリティ処理に関するテーブル（Ｓｅｃｕｒｉｔｙ　Ｐｏｌｉｃｙ　ＤａｔａｂａｓｅとＳｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ　Ｄａｔａｂａｓｅ）を検索して、当

該パケットを暗号化する必要があるか否かを判断する（ステップ６０１）。暗号化する必要がないと判断された場合、これ以降の動作は図４に示した通常のルーティング処理と同一であり、ルーティングテーブル、ＡＲＰキャッシュテーブルの検索、検索結果のＩＰフローテーブル１７への登録を実行する（ステップ４０３～４０５参照）。

〔００４９〕

パケットを暗号化する必要がある場合、マイクロプロセッサ１１は、セキュリティ処理のテーブル検索により得られた暗号化方式及び暗号鍵を含むセキュリティ情報、セキュリティ情報を識別するインデックス（ＳＰＩ）等と、カプセル化するＩＰパケットのＩＰ宛先アドレスおよびＩＰ発信元アドレスとを、セキュリティ処理部１９が接続された物理ポートを指すルーティング情報と共に、サーチ処理部１６を介してＩＰフローテーブル１７に送り、仮登録済みのＩＰフローエントリの正式登録を行う（ステップ６０２）。この動作は、図２に示すＩＰフローテーブル１７の該当ＩＰフローエントリに、出力物理ポートと、セキュリティ情報を登録することに相当する。

〔００５０〕

パケット処理部１４は、当該ＩＰフローに属するパケットに関してサーチ処理部１６によるＩＰフローテーブル１７の検索を行った際に、暗号化方式が指定されていることからＩＰｓｅｃ暗号化対象パケットであると判断する。そして、当該パケットをＩＰフローテーブル１７に指定されたＩＰ宛先アドレスとＩＰ発信元アドレスのパケットでカプセル化し、暗号化方式等のセキュリティ情報を当該カプセル化されたパケットに付加した後、指定された転送先であるセキュリティ処理部１９へ転送する（ステップ６０３）。

〔００５１〕

セキュリティ処理部１９は、受け取ったパケットからセキュリティ情報を分離し、得られたセキュリティ情報に従って当該パケットをＩＰｓｅｃ暗号化処理した後、再びパケット処理部１４へ転送する（ステップ６０４）。

〔００５２〕

パケット処理部１４は、セキュリティ処理部１９から受け取ったパケットを、

外部のネットワークインタフェースから入力されたパケットと特に区別せず、通常のパケットの様に扱ってＩＰフローテーブル１７の検索を実行する（ステップ６０５）。この際、パケットは既に新しいＩＰ宛先アドレスとＩＰ発信元アドレスでカプセル化されているため、パケット処理部１４は、新しいＩＰフローとしてＩＰフローテーブル１７へ仮登録する。

〔００５３〕

この後、マイクロプロセッサ１１がルーティング処理を行い、処理結果をＩＰフローテーブル１７へ送ってＩＰフローエントリの正式登録を行う（ステップ６０６）。当該パケットに関しては、セキュリティ処理が既に行われていることが判定可能であるため、セキュリティ処理を再実行することはない。

〔００５４〕

以上の処理を経た暗号化処理済みのパケットは、これ以降、通常のパケット同様に処理される（図３、ステップ３１３～３１５、ステップ３０７～３０９参照）。また、これ以降、当該暗号化対象のパケットと同一のサーチキー（ＩＰ発信元アドレス及びＩＰ宛先アドレス）を有するパケットを受信した場合は、対応するＩＰフローがＩＰフローテーブル１７に登録されているため、当該登録されているセキュリティ情報を用いて暗号化処理を行うことが可能である。したがって、通常のパケットに対するルーティング処理の省略と同様に、マイクロプロセッサ１１がセキュリティ情報を取得する処理を行うことなく、パケットがパケット処理部１４からセキュリティ処理部１９へ送られ、自律的に暗号化処理を実行できることとなる。

〔００５５〕

次に、図７を参照して、ＩＰｓｅｃ復号化対象パケットに対する処理について説明する。この場合、マイクロプロセッサ１１は、当該パケットのＩＰｓｅｃヘッダからＳＰＩを抽出し、これをキーとしてメインメモリ１２のセキュリティ処理のテーブル（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ　Ｄａｔａｂａｓｅ）を検索し、該当する暗号化方式、暗号鍵を得る（ステップ７０１）。次に、マイクロプロセッサ１１は、取得した暗号化方式及び暗号鍵とセキュリティ処理部１９が接続された物理ポートとを、サーチ処理部１６を介してＩＰフローテーブ

ル１７に送り、仮登録済みのＩＰフローエントリの正式登録を行う（ステップ７０２）。

〔００５６〕

パケット処理部１４は、当該ＩＰフローに属するパケットに関してサーチ処理部１６によるＩＰフローテーブル１７の検索を行った際に、暗号化方式が指定されていること及びＩＰ宛先アドレスが自装置宛であることからＩＰｓｅｃ復号化対象パケットであると判断する。そして、当該パケットに対してＩＰフローテーブル１７で指定された暗号化方式等のセキュリティ情報を付加した後、指定された転送先であるセキュリティ処理部１９へ転送する（ステップ７０３）。

〔００５７〕

セキュリティ処理部１９は、受け取ったパケットからセキュリティ情報を分離し、得られた情報に従って当該パケットをＩＰｓｅｃ復号化処理し、カプセル化されたパケットを分離した後、再びパケット処理部１４へ転送する（ステップ７０４）。

〔００５８〕

パケット処理部１４は、セキュリティ処理部１９から受け取ったパケットを、外部のネットワークインタフェースから入力されたパケットと特に区別せず、通常のパケットの様に扱ってＩＰフローテーブル１７の検索を実行する（ステップ７０５）。この際、パケットはオリジナルのＩＰ宛先アドレスとＩＰ発信元アドレスを持つパケットに復号化されているため、パケット処理部１４は新しいＩＰフローとしてＩＰフローテーブル１７へ仮登録する。

〔００５９〕

この後、マイクロプロセッサ１１がルーティング処理を行い、処理結果をＩＰフローテーブル１７へ送ってＩＰフローエントリの正式登録を行う（ステップ７０６）。ここで、当該パケットは、自装置のサブネット内のホスト宛であると判定されるため、セキュリティ処理は実行されない。

〔００６０〕

以上の処理を経た復号化処理済みのパケットは、これ以降、通常のパケット同様に処理される（図３、ステップ３１３～３１５、ステップ３０７～３０９参照

）。また、これ以降、当該復号化対象のパケットと同一のサーチキー（ＩＰ発信元アドレス及びＩＰ宛先アドレス）を有するパケットを受信した場合は、対応するＩＰフローがＩＰフローテーブル１７に登録されているため、当該登録されているセキュリティ情報を用いて復号化処理を行うことが可能である。したがって、通常のパケットに対するルーティング処理の省略と同様に、マイクロプロセッサ１１がセキュリティ情報を取得する処理を行うことなく、パケットがパケット処理部１４からセキュリティ処理部１９へ送られ、自律的に復号化処理を実行できることとなる。

〔００６１〕

以上好ましい実施形態をあげて本発明を説明したが、本発明は必ずしも上記実施形態に限定されるものではない。

〔００６２〕

例えば、上記の実施形態では、ＩＰｓｅｃの暗号化対象パケットに関して、セキュリティ処理部１９によりセキュリティ処理を行った後、当該パケットをパケット処理部１４へ戻し、パケット処理部１４において通常のパケットと同様に扱うことにより、当該パケットを下位レイヤ処理部２０へ転送しているが、このような処理に替えて、以下に示す処理を行っても良い。すなわち、パケット処理部１４が、ＩＰパケットのカプセル化、ＭＡＣヘッダの付加とセキュリティ情報を付加した後、セキュリティ処理部１９へと転送する際に、最終的な出力物理ポートの情報も付加して送出する。セキュリティ処理部１９は、パケットと共に受信した出力物理ポート情報やＭＡＣヘッダを保存しておき、パケットをＩＰｓｅｃ暗号化処理した後、パケット処理部１４を経由せずに、最終出力物理ポートと接続された下位レイヤ処理部２０へ直接転送する。

〔００６３〕

以上のような動作を行うためには、ソフトウェア制御によるマイクロプロセッサ１１の処理において、通常のルーティング処理と共にカプセル化するＩＰパケットのＩＰ宛先アドレスに基づくルーティング処理も同時に実行し、その結果をＩＰフローテーブル１７に登録するように変更すれば良い。さらにパケット処理部１４とセキュリティ処理部１９による処理も、上記動作に併せて追加すれば簡

単に実現できる。

【００６４】

以上のような動作変更を行うによって、ＩＰｓｅｃの暗号化対象パケットに対する図６に示した処理と比較して、さらなるスループットの向上を図ることができる。

【００６５】

また、上記実施形態では、マイクロプロセッサ１１が新しいＩＰフローに属するパケットのルーティング処理を行う際に、当該パケットのヘッダ部分をパケットメモリ１５の結果処理待ちキューからメインメモリ１２へコピーしていたが、このような処理に替えて、ヘッダ部分を示すパケットメモリ１５のアドレスポインタを受け取って処理を行うことも可能である。すなわち、パケット自体はパケットメモリ１５に置かれたままであり、マイクロプロセッサ１１は、当該パケットのヘッダ部分を、プロセッサバス１３及びパケット処理部１４を介して直接読み出す。

【００６６】

以上のような動作変更を行うことによって、パケットデータの転送回数が最小限に抑えられ、処理の高速化が期待できる。

【００６７】

さらに、スイッチファブリック１８としてクロスバスイッチを採用しても良い。上記実施形態におけるパケットのデータ転送は、基本的に、パケット処理部１４と各下位レイヤ処理部２０またはセキュリティ処理部１９との間における１対１に限られる。しかし、上述したようにセキュリティ処理部１９と各下位レイヤ処理部２０との間におけるパケット転送が発生する動作を行う場合は、クロスバスイッチの方がデータの衝突の頻度が少なく、全体のスループット向上が可能となる。

【００６８】

【発明の効果】

以上説明したように、本発明のパケット交換装置によれば、一度マイクロプロセッサによりルーティング処理が実行されたパケットと同一のＩＰ発信元アドレ

ス及びＩＰ宛先アドレスを有するパケットに関しては、マイクロプロセッサを用いたソフトウェア制御によるルーティング処理を行うことなくパケット交換処理を実行することができる。そのため、ＩＰパケットの転送処理の高速化を図ることができるという効果がある。

〔００６９〕

また、セキュリティのためのパケットデータの暗号化及び復号化処理を、マイクロプロセッサを用いることなく、ハードウェアにて機械的に実行することにより、セキュリティ処理の高速化を図ることができるという効果がある。

〔００７０〕

また、ＩＰフローテーブルを用いてマイクロプロセッサのルーティング処理を行わないパケット転送を実現する構成と、セキュリティ処理を実行するハードウェアとを組み合わせることにより、従来のパケット交換装置と比較して、ネットワークレイヤでのセキュリティ処理を伴うパケット交換を、非常に高速に行うことができる。

〔００７１〕

さらに、セキュリティ処理を行うハードウェアをスイッチファブリックの一構成ユニットとすることにより、セキュリティ処理の独立性を高めることができる。これにより、パケット交換装置へのセキュリティ処理機能の追加や、暗号方式の変更及び追加が容易となるため、パケット交換装置における装置構成の柔軟性及び拡張性の向上を図ることができる。

〔図面の簡単な説明〕

〔図１〕　本発明の一実施形態によるパケット交換装置の構成を示すブロック図である。

〔図２〕　本実施形態におけるＩＰフローテーブルの例を示す図である。

〔図３〕　本実施形態におけるパケット処理の主要な流れを示すフローチャートである。

〔図４〕　本実施形態におけるマイクロプロセッサのルーティング処理の流れを示すフローチャートである。

〔図５〕　本実施形態におけるセキュリティ処理を伴うパケット処理の流れ

を示すフローチャートであり、マイクロプロセッサがパケットの種類を認識するまでの動作を示す図である。

【図６】　本実施形態におけるセキュリティ処理を伴うパケット処理の流れを示すフローチャートであり、ＩＰｓｅｃ暗号化対象パケットに対する処理を示す図である。

【図７】　本実施形態におけるセキュリティ処理を伴うパケット処理の流れを示すフローチャートであり、ＩＰｓｅｃ復号化対象パケットに対する処理を示す図である。

【図８】　ＩＰｓｅｃトンネルモードによって処理されたＩＰパケットの構成を示す図である。

【図９】　従来のパケット交換装置の構成を示すブロック図である。

【符号の説明】

１１　　マイクロプロセッサ

１２　　メインメモリ

１３　　プロセッサバス

１４　　パケット処理部

１５　　パケットメモリ

１６　　サーチ処理部

１７　　ＩＰフローテーブル

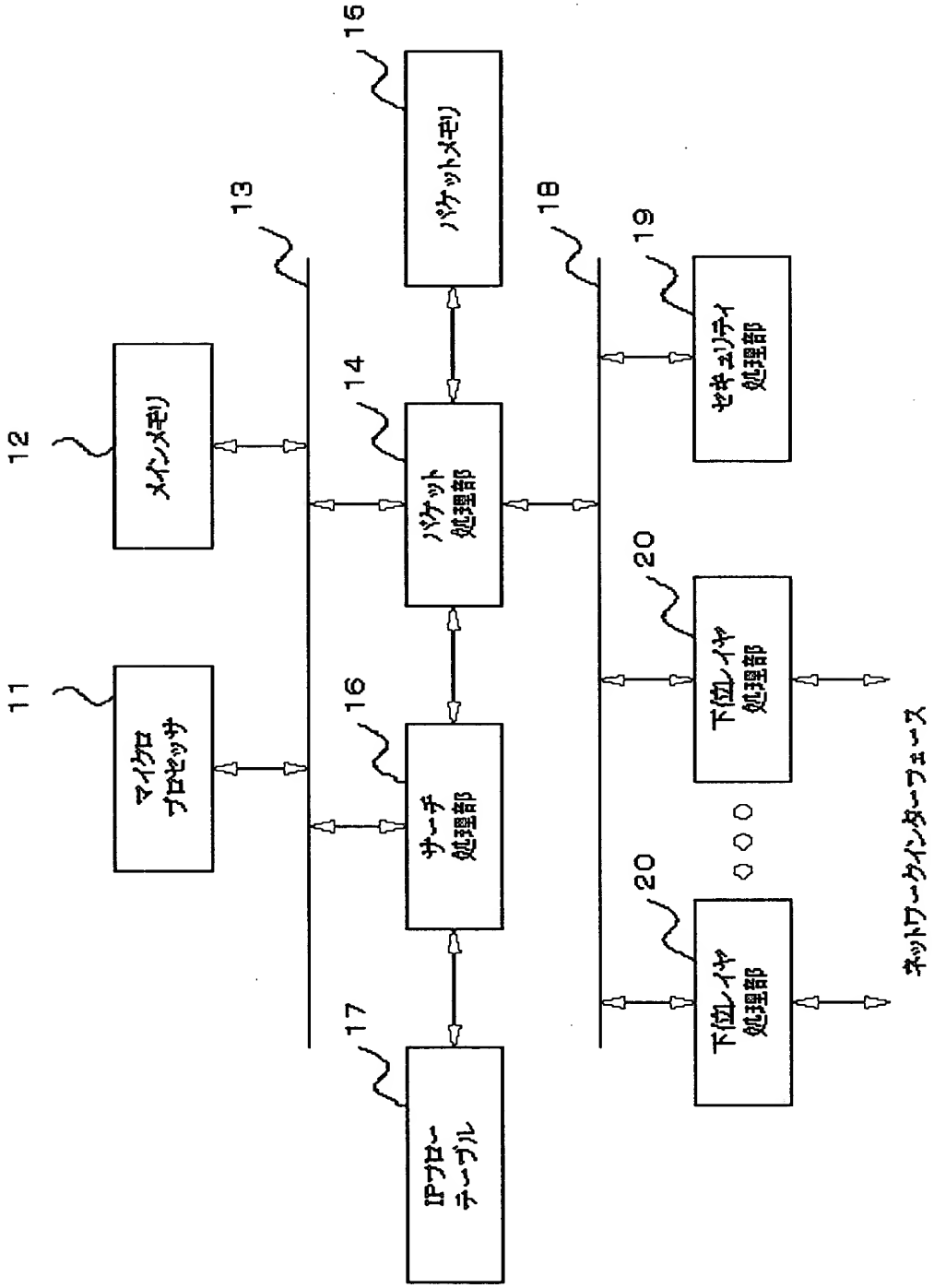
１８　　スイッチファブリック

１９　　セキュリティ処理部

２０　　下位レイヤ処理部

【書類名】　　図面

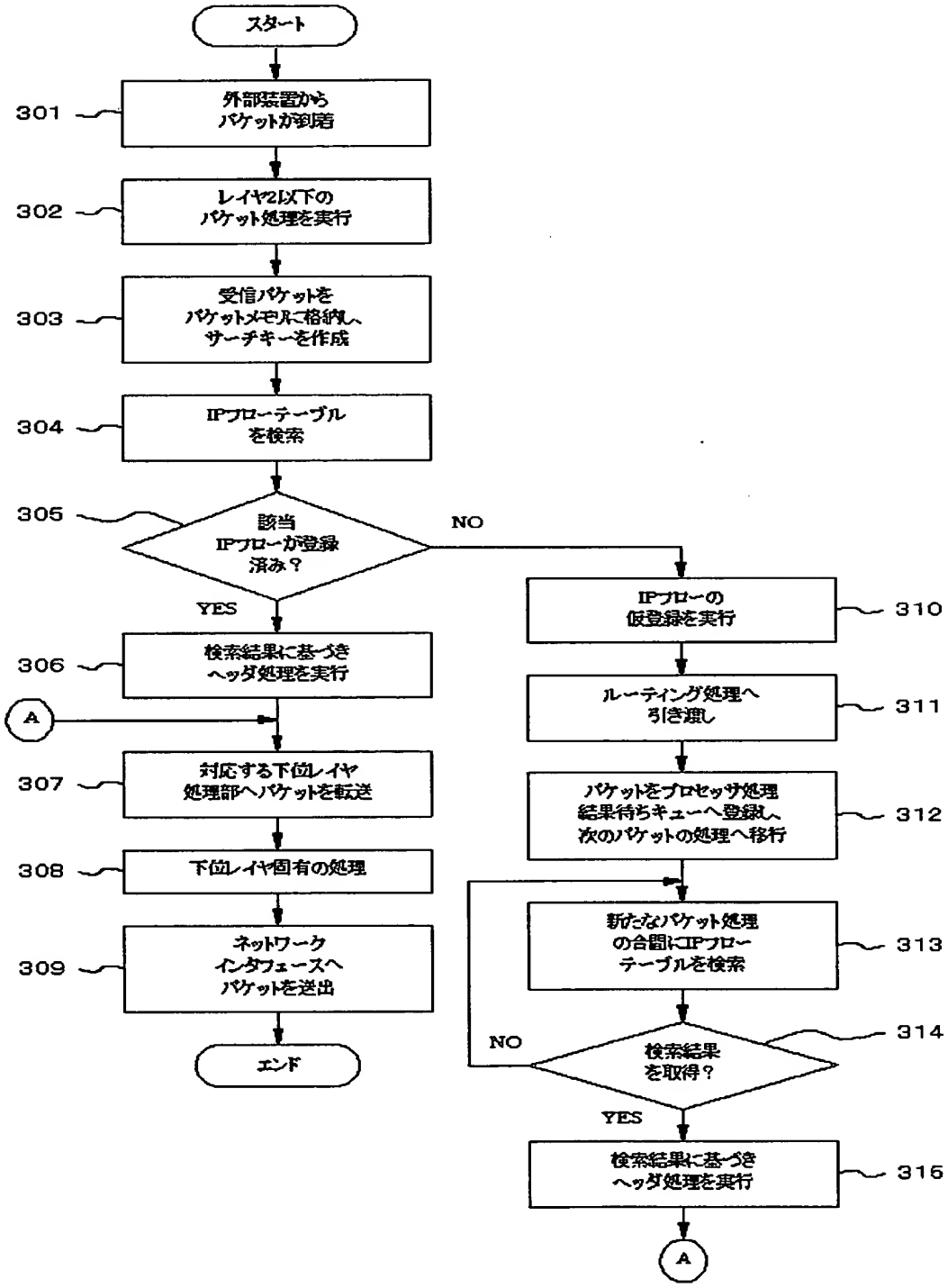
【図１】


16
パケットメモリ
13
18
19
セキュリティ
処理部
12
メインメモリ
14
パケット
処理部
20
下位レイヤ
処理部
11
マイクロ
プロセッサ
16
サーチ
処理部
20
下位レイヤ
処理部
17
IPフロー
テーブル
ネットワークインターフェース

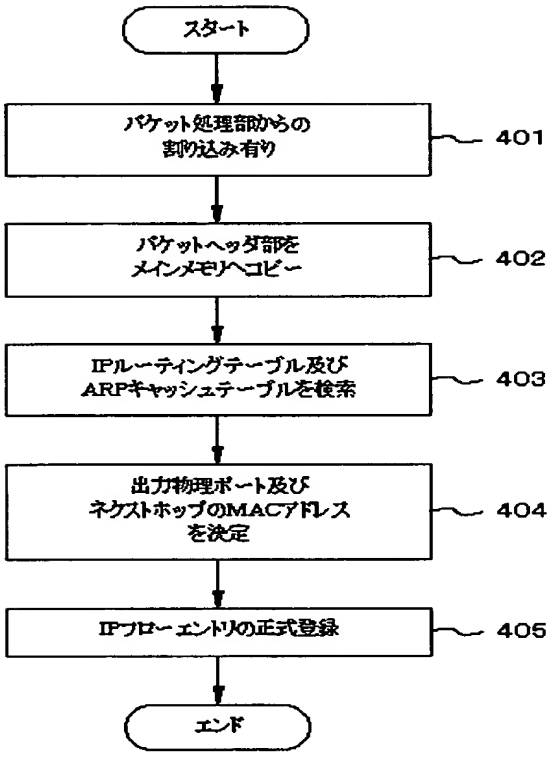
【図２】

サーチキー		ルーティング結果			セキュリティ情報				
IP Source Address	IP Destination Address	MAC Source Address	MAC Destination Address	Output Port No.	Encryption Algorithm	Encryption Key	New IP Source Address	New IP Destination Address
AA BB CC DD	EE FF GG HH	123456	789012	2				
AA BB CC DD	KK LL MM NN			9	DES-CBC	XXXXXX	AA BB CC XX	KK LL MM YY
AA BB CC XX	KK LL MM YY	123456	789012	2				
KK LL MM YY	AA BB CC XX			9	DES-CBC	YYYYYY		
*** ***	*** ***	*** ***	*** ***	*** ***	*** ***	*** ***	*** ***	*** ***

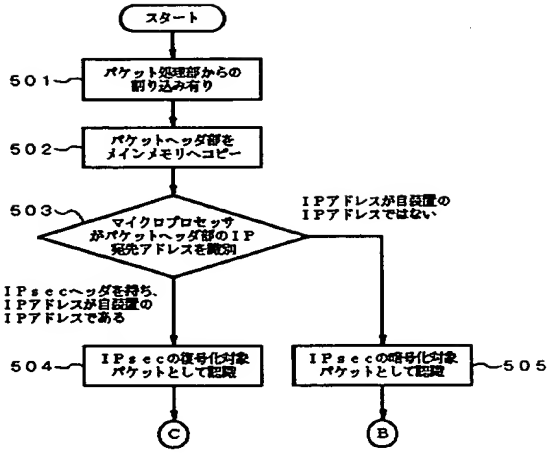
【図３】


スタート
301
外部装置から
パケットが到着
302
レイヤ2以下の
パケット処理を実行
303
受信パケットを
パケットメモリに格納し、
サーチキーを作成
304
IPフローテーブル
を検索
305
該当
IPフローが登録
済み？
NO
YES
306
検索結果に基づき
ヘッダ処理を実行
A
307
対応する下位レイヤ
処理部へパケットを転送
308
下位レイヤ固有の処理
309
ネットワーク
インタフェースへ
パケットを送出
エンド
310
IPフローの
仮登録を実行
311
ルーティング処理へ
引き渡し
312
パケットをプロセッサ処理
結果待ちキューへ登録し、
次のパケットの処理へ移行
313
新たなパケット処理
の合間にIPフロー
テーブルを検索
314
検索結果
を取得？
NO
YES
316
検索結果に基づき
ヘッダ処理を実行
A

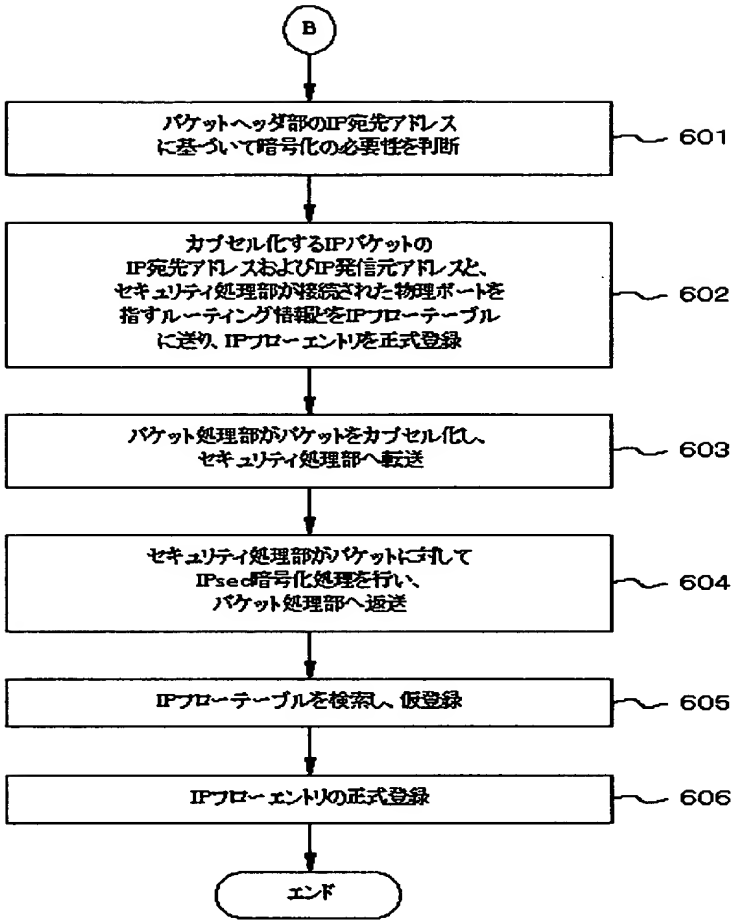
【図４】


スタート
パケット処理部からの
割り込み有り
401
パケットヘッダ部を
メインメモリへコピー
402
IPルーティングテーブル及び
ARPキャッシュテーブルを検索
403
出力物理ポート及び
ネクストホップのMACアドレス
を決定
404
IPフローエントリの正式登録
405
エンド

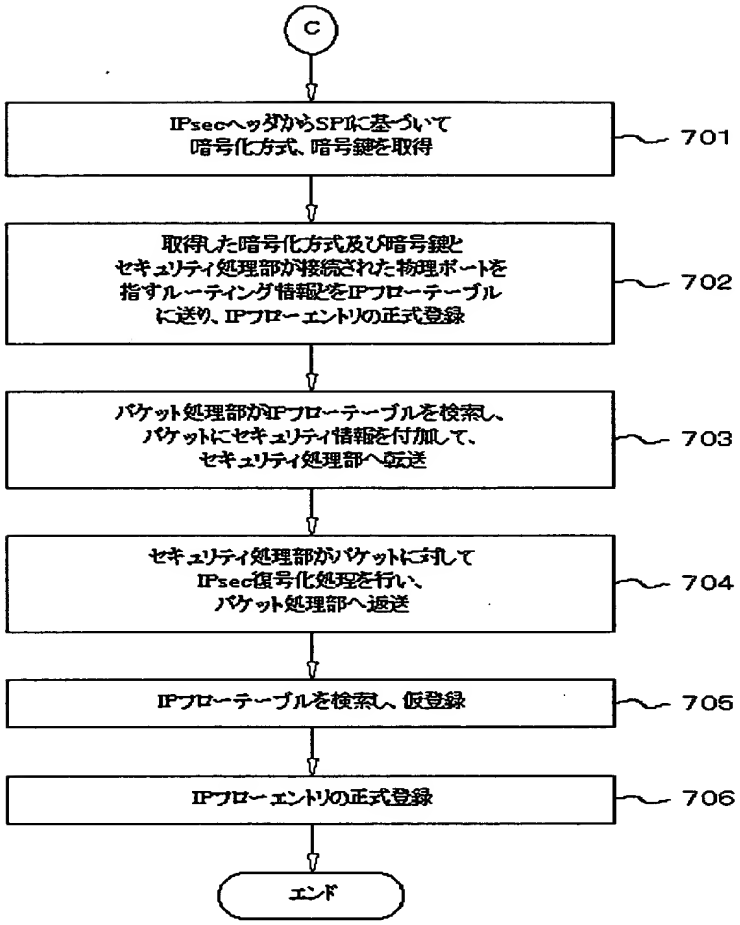
【図５】


スタート
501
パケット処理部からの
割り込み有り
502
パケットヘッダ部を
メインメモリへコピー
503
マイクロプロセッサ
がパケットヘッダ部のＩＰ
宛先アドレスを識別
ＩＰアドレスが自装置の
ＩＰアドレスではない
ＩＰｓｅｃヘッダを持ち、
ＩＰアドレスが自装置の
ＩＰアドレスである
504
ＩＰｓｅｃの復号化対象
パケットとして認識
ＩＰｓｅｃの暗号化対象
パケットとして認識
505
C
B

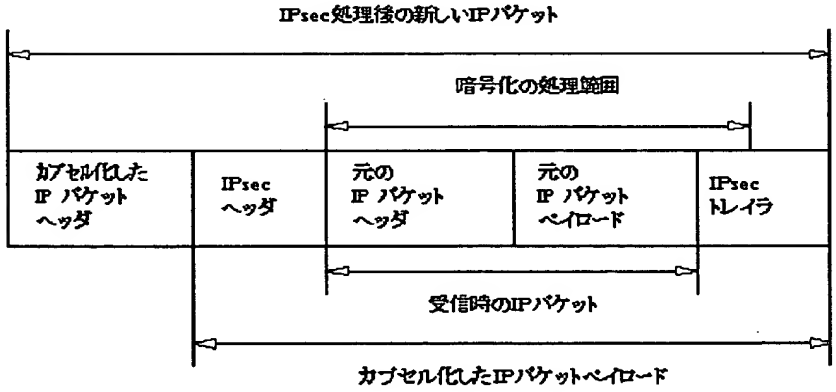
【図６】


B
パケットヘッダ部のIP宛先アドレス
に基づいて暗号化の必要性を判断
601
カプセル化するIPパケットの
IP宛先アドレスおよびIP発信元アドレスと、
セキュリティ処理部が接続された物理ポートを
指すルーティング情報をIPフローテーブル
に送り、IPフローエントリを正式登録
602
パケット処理部がパケットをカプセル化し、
セキュリティ処理部へ転送
603
セキュリティ処理部がパケットに対して
IPsec暗号化処理を行い、
パケット処理部へ返送
604
IPフローテーブルを検索し、仮登録
605
IPフローエントリの正式登録
606
エンド

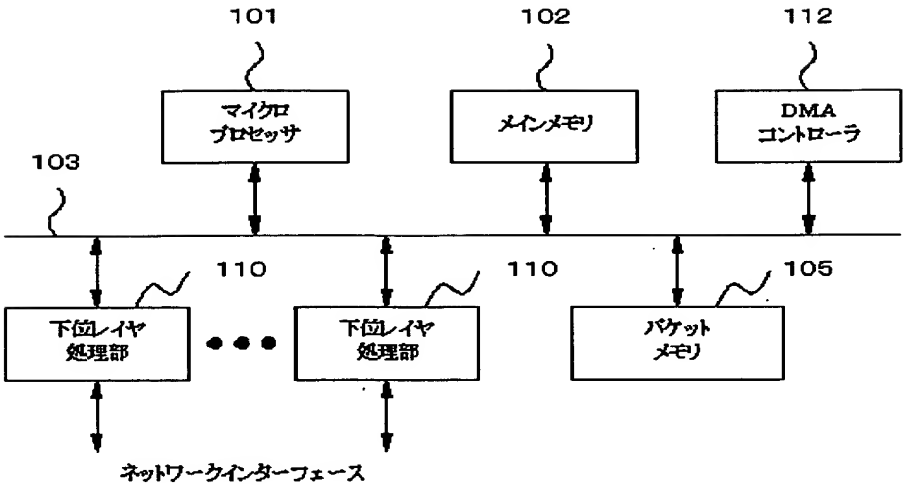
【図７】


C
IPsecヘッダからSPIに基づいて
暗号化方式、暗号鍵を取得
701
取得した暗号化方式及び暗号鍵と
セキュリティ処理部が接続された物理ポートを
指すルーティング情報をIPフローテーブル
に送り、IPフローエントリの正式登録
702
パケット処理部がIPフローテーブルを検索し、
パケットにセキュリティ情報を付加して、
セキュリティ処理部へ転送
703
セキュリティ処理部がパケットに対して
IPsec復号化処理を行い、
パケット処理部へ返送
704
IPフローテーブルを検索し、仮登録
705
IPフローエントリの正式登録
706
エンド

【図８】


IPsec処理後の新しいIPパケット
暗号化の処理範囲
カプセル化した
IP パケット
ヘッダ
IPsec
ヘッダ
元の
IP パケット
ヘッダ
元の
IP パケット
ペイロード
IPsec
トレイラ
受信時のIPパケット
カプセル化したIPパケットペイロード

【図９】


101
102
112
マイクロ
プロセッサ
メインメモリ
DMA
コントローラ
103
110
110
105
下位レイヤ
処理部
下位レイヤ
処理部
パケット
メモリ
ネットワークインターフェース

【書類名】　　要約書

【要約】

【課題】　ルーティング処理及びセキュリティ処理におけるマイクロプロセッサの負担を軽減することにより、パケット交換処理の高速化を実現するパケット交換装置を提供する。

【解決手段】　パケット通信ネットワークに用いられ、パケット単位でルーティング処理を実行しパケット転送を行うパケット交換装置において、ソフトウェア制御により受信パケットのルーティング処理を行うマイクロプロセッサと、前記マイクロプロセッサによりルーティング処理がなされたパケットに関して、ＩＰ発信元アドレスとＩＰ宛先アドレスとをサーチキーとして、ルーティング処理の結果を登録し、保持するＩＰフローテーブルと、パケットを受信した場合に、該受信パケットのＩＰ発信元アドレス及びＩＰ宛先アドレスをサーチキーとして前記ＩＰフローテーブルを検索し、検索の結果、該当するＩＰフローが登録されていた場合、前記マイクロプロセッサによるルーティング処理へ移行することなく、該ＩＰフローに示されるルーティング処理結果に基づいて、該パケットを適切な出力ポートへ転送するパケット処理実行手段と、ネットワークインタフェースと接続され、受信したパケットに対して下位レイヤの処理を実行して前記パケット処理実行手段に転送し、前記パケット処理実行手段から受け取ったパケットに対して下位レイヤの処理を実行してネットワークへ送出する下位レイヤ処理手段とを備える。

【選択図】　　図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第０９８１４０号
受付番号	５９９００３２１５７６
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１１年　４月１５日

＜認定情報・付加情報＞

【提出日】　平成11年 4月 5日

次頁無

出証特２０００－３０１４２８４

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社